BURMISTRZ GŁUSZYCY
ul. Parkowa 9, 58-340 Głuszyca

Zarządzenie nr 3/O/2025
Burmistrza Głuszycy

z dnia 7 stycznia 2025 r.

w sprawie wprowadzenia dokumentów dotyczących Ochrony Danych Osobowych w Urzędzie Miejskim w Głuszycy

Na podstawie art. 33 ust. 1 i ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2024 r., poz.1465 z późn. zm.) oraz art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) zarządzam, co następuje:

§ 1. Wprowadza się dokumenty dotyczące Ochrony Danych Osobowych w Urzędzie Miejskim w Głuszycy, stanowiące odpowiednio Załączniki do niniejszego Zarządzenia:

1) Regulamin Ochrony Danych Osobowych – Załącznik Nr 1
2) Instrukcje postępowania w sytuacji naruszenia systemu ochrony danych osobowych – Załącznik nr 2
3) Rejestr naruszeń ochrony danych osobowych – Załącznik nr 3
4) Rejestr udostępnień – Załącznik nr 4

§ 2. Zobowiązuję wszystkich pracowników Urzędu Miejskiego do zapoznania się i przestrzegania niniejszego Zarządzenia.

§ 3. Traci moc Zarządzenie nr 17/O/2022 Burmistrza Głuszycy z dnia 9 marca 2022 r. w sprawie wprowadzenia Regulaminu Ochrony Danych Osobowych, załączników do Regulaminu, Instrukcji postępowania w sytuacji naruszenia systemu danych osobowych, rejestru udostępnień oraz rejestru naruszeń.

§ 4. Wykonanie Zarządzenia powierza się Inspektorowi Ochrony Danych (IOD).

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ GŁUSZYCY

UZASADNIENIE

Z uwagi na liczne zmiany w dokumentacji dotyczące Ochrony Danych Osobowych w Urzędzie Miejskim w Głuszycy, należało zaktualizować posiadane dokumenty i ujednolicić je w nowym Zarządzeniu, stąd jego podjęcie jest zasadne.

Zał. Nr 1 do Zarządz. Bm
Nr 3/01/2025 z 7.01.25 r.

Regulamin Ochrony Danych Osobowych

Nazwa podmiotu wprowadzającego	Urząd Miejski w Głuszycy
Data wprowadzenia	3/2025
Numer zarządzenia wprowadzającego	7 stycznia 2025 r.
Podpis ADO	
Podpis IOD	Chata Michajec Aleksandra

1. WSTĘP:

§1

Regulamin Ochrony Danych Osobowych stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad dotyczących ochrony danych osobowych dla pracowników, współpracowników oraz innych osób przetwarzających dane osobowe administratora.

§2

Regulamin Ochrony Danych Osobowych został opracowany zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (dalej „RODO"), a także ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

§3

Regulamin Ochrony Danych Osobowych stosuje się do danych osobowych przetwarzanych w systemach informatycznych, danych osobowych zapisanych na zewnętrznych nośnikach informacji, a także danych przetwarzanych w sposób tradycyjny.

§4

Każda osoba przetwarzająca dane administratora zobowiązana jest do zapoznania się z poniższym regulaminem ochrony danych osobowych oraz stosowaniem procedur i zasad w nim zawartych.

2. DEFINICJE:

Przez użyte w Regulaminie Ochrony Danych Osobowych określenia należy rozumieć:

1. **Regulamin** - Regulamin Ochrony Danych Osobowych, zwany inaczej Polityką Bezpieczeństwa Ochrony Danych Osobowych,
2. **Administrator Danych Osobowych (ADO)** - podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
3. **Inspektor Ochrony Danych Osobowych (IOD)** - osoba lub podmiot wspierający administratora danych w realizacji obowiązków dotyczących ochrony danych osobowych oraz realizujący zadania, wynikające z art. 39 RODO.
4. **RODO** - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (dalej „RODO"),
5. **Ustawa** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
6. **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
7. **Zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
8. **Przetwarzanie danych** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany; taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnienie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowanie lub łączenie, ograniczenie, usuwanie lub niszczenie, przechowywanie, adaptowanie lub modyfikowanie.
9. **Usuwanie danych** - zniszczenie danych lub ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą,
10. **Zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie swoich danych osobowych,
11. **Naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

3. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH:

1. Dane osobowe w jednostce należy:
   a) przetwarzać zgodnie z prawem, rzetelnie i w sposób przejrzysty (zgodność z prawem, rzetelność i przejrzystość),
   b) zbierać w konkretnych, wyraźnych i prawnie uzasadnionych celach (ograniczenie celu),
   c) ograniczać do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych),
   d) uaktualniać w razie potrzeby; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (prawidłowość),
   e) przechowywać w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne (ograniczenie przechowywania),
   f) przetwarzać w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych; w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (integralność i poufność),
2. Dane osobowe w jednostce przetwarzane są zgodnie z prawem, jeżeli:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów np. w celach promocyjnych,
   b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą np. zawieranie umowy o pracę z pracownikami,
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
   d) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
   e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.
3. Dane osobowe szczególnej kategorii przetwarzane są w jednostce zgodnie z prawem, jeżeli:
   a) Osoba, której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie danych osobowych w jednym lub kilku konkretnych celach,
   b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,

c) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,

d) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy,

e) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi.

4. OBOWIĄZKI ADMINISTRATORA ORAZ INSPEKTORA OCHRONY DANYCH OSOBOWYCH:

1. Administrator Danych Osobowych:
   a) zobowiązany jest do wdrożenia środków fizycznych, technicznych oraz organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych,
   b) realizuje zasady przetwarzania danych osobowych za które jest odpowiedzialny i potrafi wykazać ich przestrzeganie (rozliczalność),
   c) prowadzi i aktualizuje dokumentacje opisującą sposób przetwarzania danych oraz zapewniającą ochronę danych i bezpieczeństwo ich przetwarzania,
   d) nadaje upoważnienia do przetwarzania danych dla osób przetwarzających jego dane osobowe oraz zapoznaje wszystkich pracowników z niniejszym regulaminem.
   e) organizuje szkolenia z zakresu ochrony danych osobowych dla pracowników oraz innych osób przetwarzających dane,
   f) współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
   g) zgłasza naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadamia osoby, których dane dotyczą o naruszeniu ich danych osobowych, zgodnie z wprowadzonymi procedurami.
   h) wyznacza Inspektora Ochrony Danych Osobowych.
2. Administrator Danych Osobowych wyznaczył Inspektora Ochrony Danych Osobowych.
3. Inspektorem Ochrony Danych Osobowych jest Aleksandra Cnota-Mikołajec z którą można skontaktować się za pomocą telefonu komórkowego: 500 325 811 oraz adresu mailowego; aleksandra@eduodo.pl,
4. Inspektor Ochrony Danych Osobowych jest odpowiedzialny w szczególności za:
   a) monitorowanie przestrzegania przepisów dotyczących ochrony danych osobowych oraz niniejszego regulaminu,
   b) udzielanie zaleceń co do oceny skutków dla ochrony danych,
   c) współpracę z organami ochrony danych i pełnieniem funkcji punktu kontaktowego dla organów ochrony danych w kwestiach związanych z przetwarzaniem,

d) przygotowanie oraz aktualizację dokumentacji z zakresu ochrony danych osobowych.

5. NADAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH:

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu upoważnienia do przetwarzania danych osobowych,
2. Przed przystąpieniem do przetwarzania danych osobowych należy zapoznać się z przepisami o ochronie danych osobowych, materiałem informacyjnym dla osób przetwarzających dane osobowe oraz dokumentacją dotyczącą ochrony danych osobowych wprowadzoną przez administratora,
3. Proces nadawania upoważnień do przetwarzania danych osobowych odbywa się w wersji papierowej,
4. Upoważnienia do przetwarzania danych osobowych przygotowuje Inspektor Ochrony Danych,
5. Upoważnienia do przetwarzania danych osobowych akceptuje i podpisuje Administrator Danych Osobowych.
6. Upoważnienie przygotowuje się zgodnie i z odniesieniem do zakresu czynności, jakie wykonuje dana osoba,
7. Upoważnienia do przetwarzania danych osobowych przechowywane są w aktach osobowych danego pracownika oraz w teczce zawierającej dokumentacja dotyczącą ochrony danych osobowych,
8. Upoważnienia do przetwarzania danych osobowych zgodnie z zapisem zawartym w upoważnieniu wygasają z chwilą ustania zatrudnienia lub funkcji.

6. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH:

1. Każda osoba dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a) przetwarzania danych osobowych wyłącznie w zakresie i celach przewidzianych w zadaniach powierzonych przez administratora,
   b) zachowania tajemnicy przetwarzanych danych osobowych w związku z wykonywaniem zadań powierzonych przez administratora,
   c) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   d) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Każda osoba dopuszczona do przetwarzania danych zobowiązuje się do niewykorzystywania danych osobowych w celach niezgodnych z zakresem oraz celem powierzonych zadań,

3. Osobom dopuszczonym do przetwarzania danych osobowych zabrania się przekazywania, bezpośrednio lub przez telefon danych osobowych, osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować,
4. Każda osoba dopuszczona do przetwarzania danych osobowych zapoznaje się z przepisami o ochronie danych osobowych oraz niniejszym regulaminem.

7. ZABEZPIECZENIA DOKUMENTACJI PAPIEROWEJ:

1. Osoby upoważnione do przetwarzania danych odpowiedzialne są za bezpieczeństwo dokumentów i wydruków,
2. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zamykania dokumentów na klucz w szafach, biurkach, sejfach podczas ich nieobecności w pomieszczeniach lub po zakończeniu swojej pracy (tzw. polityka czystego biurka),
3. Pomieszczenia, w których przetwarzane są dane osobowe muszą być każdorazowo zamykane na klucz,
4. Zabrania się pozostawiania kluczy w zamkach drzwi (od wewnątrz i od zewnątrz),
5. Zabrania się pozostawiania kluczy w zamkach szaf i biurek po godzinach pracy lub podczas ich nieobecności. Klucze należy zabezpieczyć i chować w miejsce niedostępne dla osób nieuprawnionych. Za takie miejsce nie uznaje się pierwszej szuflady w biurku,
6. Osoby upoważnione zobowiązane są do niszczenia dokumentów i tymczasowych wydruków niezwłocznie po ustaniu ich przydatności w niszczarkach,
7. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami np. w korytarzach, pomieszczeniach konferencyjnych,
8. Zabrania się pozostawiania ksero oraz wydruków, zawierających dane osobowe na urządzeniach np. drukarce, kserokopiarce,
9. Zabrania się wywieszania danych osobowych w miejscach widocznych dla osób postronnych; w tym tablicach korkowych,
10. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz np. terenach publicznych, lasach itp.
11. Zabrania się zabierania dokumentów w domu w celu utylizacji ich w prywatnych systemie grzewczym np. piec, kominek.

8. ZASADY WYNOSZENIA DOKUMENTÓW POZA JEDNOSTKĘ:

1. Osoby upoważnione nie mogą wynosić dokumentacji papierowej na zewnątrz jednostki bez pisemnej zgody administratora,
2. Administrator Danych Osobowych zapewnia ewidencjonowanie wydanych pracownikom dokumentów, zawierających dane osobowe,

3. Liczba wynoszonych dokumentów z siedziby administratora jest ograniczona do tego, co niezbędne w stosunku do celów przetwarzania danych osobowych przez pracownika w ramach pracy,
4. Osoby upoważnione zobowiązują się do odpowiedniego zabezpieczenia danych osobowych podczas ich wynoszenia np. wynoszenie dokumentów w aktówce. Dokumenty należy przenosić w taki sposób, aby była ona niewidoczna dla osób trzecich,
5. Osoby upoważnione wykonujące pracę w domu zobowiązują się do odpowiedniego zabezpieczenia danych w miejscu wykonywania pracy. Przestrzegają zasady czystego biurka oraz zabezpieczają dokumentacje przed wglądem osób nieuprawnionych np. domowników.
6. Osoby upoważnione wykonujące pracę w domu zobowiązują się do przechowywania dokumentacji w zamykanych na klucz szafach do których wyłącznie on ma dostęp,
7. Administrator Danych Osobowych korzysta wyłącznie ze sprawdzonych firm kurierskich. W przypadku, gdy dokumenty przewozi pracownik, zobowiązuje się on do zabezpieczania przewożonych dokumentów przed zgubieniem, kradzieżą, zniszczeniem itd.

9. UDOSTĘPNIANIE DANYCH OSOBOWYCH:

1. Administrator zobowiązany jest do prowadzenia rejestru udostępnień danych osobowych,
2. Dane osobowe udostępniane są na pisemny wniosek z uwzględnieniem podstawy prawnej do ich udostępnienia, chyba, że przepis innej ustawy stanowi inaczej,
3. Wniosek o udostępnienie danych musi zawierać:
   a) nazwę jednostki organizacyjnej lub imię i nazwisko osoby, której udostępniane są dane,
   b) termin, podstawę prawną oraz zakres udostępnianych danych,
4. Wnioski o udostępnienie danych osobowych mogą być przyjmowane przez każdą osobę upoważnioną,
5. Każdy otrzymany wniosek o udostępnienie danych należy przekazać administratorowi lub inspektorowi ochrony danych osobowych.

10. ZABEZPIECZENIE SPRZĘTU IT ORAZ NOŚNIKÓW ZEWNĘTRZNYCH:

1. Użytkownik zobowiązany jest do ochrony sprzętu IT przed jakimkolwiek zniszczeniem lub uszkodzeniem. Sprzętem IT jest: komputer stacjonarny, laptop, monitor, drukarka, skaner, tablet, smartfon i nośniki zewnętrzne, którymi są: dyski twarde, płyty CD/DVD, pendrive, pamięć typu „flash" itp.
2. Każdy użytkownik zobowiązany jest do natychmiastowego zgłoszenia zagubienia, utraty, awarii lub zniszczenia powierzonego mu sprzętu IT,
3. Zabrania się samodzielnego demontażu sprzętu IT, instalowania dodatkowych urządzeń np. twardych dysków, instalowania oprogramowania bez wiedzy administratora lub podłączenia

jakichkolwiek niezatwierdzonych przez administratora urządzeń np. smartfonów, pendrive do systemu informatycznego.

4. Zabrania się umożliwiania osobom nieuprawnionym wglądu do danych wyświetlanych na monitorach komputerowych.
5. Monitory komputerów oraz laptopów muszą być odwrócone w sposób uniemożliwiający wgląd osobom nieupoważnionym.
6. Zabrania się dopuszczania osób nieupoważnionych do sprzętu IT.
7. Przed odejściem od stanowiska pracy, użytkownik zobowiązany jest do każdorazowego blokowania hasłem komputera (skrót klawiszowy: WINDOWS+L) oraz wylogowania się ze wszystkich programów, w których przetwarzane są dane osobowe,
8. Po zakończeniu pracy użytkownik zobowiązuje się do wylogowania się z systemu informatycznego oraz wyłączenia sprzętu komputerowego,
9. Nośniki danych są przechowywane w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym oraz w miejscu zabezpieczającym przed zagrożeniami tj. zalanie, pożar, wpływ pól elektromagnetycznych,
10. Użytkownicy zobowiązani są do niezwłocznego i trwałego usuwania danych osobowych z nośników zewnętrznych po ustaniu powodu ich przechowywania, chyba, że przepisy odrębne stanowią inaczej,
11. Użytkownicy zobowiązani są do niezwłocznego i trwałego usuwania plików z nośników zewnętrznych do których mają także dostęp nieupoważnieni użytkownicy.

11. NISZCZENIE NOŚNIKÓW ZEWNĘTRZNYCH:

1. Niszczenie nośników zewnętrznych oznacza takie uszkodzenie mechaniczne, które uniemożliwia odzysk zapisanych na nich informacji,
2. Niszczeniu podlegają nośniki zewnętrzne dla których minął okres ich ważności, nie przewiduje się ich dalszego użytkowania (chyba, że przepisy odrębne stanowią inaczej) lub istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać przechowywania informacji,
3. Niszczenie nośników zewnętrznych odbywa się na polecenie Administratora Danych Osobowych oraz za wiedzą Inspektora Ochrony Danych Osobowych,
4. Niszczenie dokonuje się w sposób następujący:
    - dyski twarde rozbiera się na części i niszczy talerze dysku,
    - płyty przełamuje się na kilka części lub korzysta z niszczarki,
    - taśmy magnetyczne wyciąga się z obudowy i przecina na części,
    - dyskietki przełamuje się na kilka części,
    - karty procesorowe przełamuje się, należy zwrócić uwagę, aby zniszczyć procesor.
5. Po zakończeniu niszczenia sporządzony zostaje rejestr likwidacji nośników.

12. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ:

1. Przesyłanie danych osobowych za pomocą poczty elektronicznej może odbywać się tylko przez osoby upoważnione,
2. Przesyłając dane osobowe należy wykorzystywać mechanizmy kryptograficzne,
3. Hasło zabezpieczające wysyłane pliki musi się składać się z minimum osiem znaków; w tym duże i małe litery, oraz cyfry lub znaki specjalne. Hasło należy przesłać inną metodą np. telefonicznie. Zabrania się przesyłania hasła na ten sam adres e-mail,
4. Użytkownicy zobowiązani są do zwracania szczególnej uwagi na poprawność adresu odbiorcy dokumentu. Zaleca się, aby w treści wysyłanej wiadomości zawrzeć prośbę o potwierdzenie otrzymania maila.
5. Zabrania się otwierania plików (załączników) bez weryfikacji nadawcy. Tego typu maile mogą zawierać załączniki ze szkodliwym oprogramowaniem, które infekują komputer użytkownika, czego skutkiem jest utrata danych osobowych.
6. Zabrania się otwierania linków w mailach bez weryfikacji nadawcy, gdyż mogą to być odnośniki do stron zainfekowanych lub niebezpiecznych. Wchodząc na tego typu linki użytkownik infekuje komputer oraz pozostałe komputery w sieci.
7. Każdy przypadek wykrycia podejrzanych wiadomości należy zgłosić administratorowi i inspektorowi ochrony danych osobowych,
8. Użytkownikom nie wolno rozsyłać maili niezwiązanych z pracą w formie „łańcuszków szczęścia",
9. Wysyłając maile do wielu adresatów należy użyć opcji „ukryta kopia". Zabrania się rozsyłania wiadomości do wielu adresatów z użyciem „do wiadomości",
10. Użytkownicy muszą kasować niepotrzebne maila minimum raz w miesiącu,
11. Zabrania się używania danych osobowych lub poufnych informacji w temacie wiadomości,
12. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych. Użytkownicy mogą skorzystać z poczty mailowej do celów prywatnych wyłącznie w nagłych przypadkach i za zgodą administratora,
13. Zabrania się uruchamiania przekierowania wiadomości ze służbowej skrzynki mailowej na prywatną,
14. Użytkownicy korzystający z maila zobowiązani są do przestrzegania prawa własności przemysłowej i prawa autorskiego,
15. Zabrania się korzystania z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania,
16. Użytkownik bez zgody administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe administratora, jego pracowników, klientów, dostawców, kontrahentów za pośrednictwem Internetu; w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

17. Użytkownicy nie wykorzystują komunikatorów dostępnych w sieciach oraz usługach społecznościowych w celach służbowych,
18. Każdy użytkownik jest odpowiedzialny za tekstową, dźwiękową lub graficzną treść wysyłanych wiadomości.

13. KORZYSTANIE Z INTERNETU:

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych,
2. Zabrania się zgrywania na dysk twardy komputera, instalowania oraz uruchamiania programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki można pobrać wyłącznie za zgodą ADO i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu,
4. Zabrania się wchodzenia na strony internetowe, które prezentują informacje o charakterze przestępczym, pornograficznym, innym zakazanym przez prawo, gdyż na większości tych stron jest zainstalowane szkodliwe oprogramowanie, które w sposób automatyczny infekuje system operacyjny komputera.
5. Zabrania się włączania opcji autouzupełniania formularzy i zapamiętywania haseł w przeglądarce,
6. Podczas korzystania z zaszyfrowanego przez przeglądarkę połączenia, każdy użytkownik zobowiązany jest do sprawdzenia czy połączenie jest zabezpieczone. Należy zwrócić uwagę na ikonę kłódki oraz adresu internetowego rozpoczynającego się od „https". Dla pewności należy kliknąć ikonę kłódki, aby sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel,
7. Użytkownicy muszą zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę internetową np. banku, e-sklepu, poczty mailowej, a także w przypadku podania loginów, haseł, PIN-ów, numerów kart płatniczych za pomocą Internetu. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank,
8. Użytkownicy mogą korzystać z Internetu w celach prywatnych wyłącznie okazjonalnie i za zgodą administratora. Korzystanie z Internetu w celach prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego administratora,
9. Użytkownicy korzystający z Internetu zobowiązani są do przestrzegania prawa własności przemysłowej i prawa autorskiego,
10. Administrator Danych Osobowych zastrzega sobie prawo do kontrolowania sposobu korzystania przez użytkownika z Internetu w zakresie dozwolonym przepisami prawa,
11. Administrator Danych Osobowych zastrzega sobie prawo do kontrolowania czasu spędzonego przez użytkownika w Internecie w uzasadnionym zakresie,

12. Administrator Danych Osobowych ma prawo blokować dostęp do niektórych treści dostępnych w Internecie.

14. ZARZĄDZANIE UPRAWNIENIAMI:

1. Każdy użytkownik mający dostęp do danych osobowych w systemie informatycznym np. na dysku sieciowym, programie oraz poczcie elektronicznej musi posiadać własny identyfikator (login) do logowania się. Wyjątek stanowi konto użytkownika w systemie Windows,
2. Osobą odpowiedzialną za nadawanie uprawnień jest administrator danych osobowych lub administrator systemów informatycznych. Nadany login oraz pierwsze hasło podawane są w formie ustnej,
3. Każdy użytkownik zobowiązany jest do niezwłocznej zmiany hasła po jego otrzymaniu,
4. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia tylko na wyraźne polecenie administratora i przy realizacji administratorów systemów informatycznych,
5. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień np. przydzielenia sobie uprawnień administratora w systemie, tworzenia kont gościa itd.,
6. Użytkownicy zobowiązani są do pracy na własnym koncie. Zabronione jest umożliwianie pracy na koncie i przekazywanie danych dostępowych w postaci loginu oraz hasła innym użytkownikom.

15. POLITYKA HASEŁ:

1. Hasła nie mogą być powszechnie używanymi słowami. Zabrania się wykorzystywania dat narodzin, ślubu oraz innych ważnych wydarzeń, imion i nazwisk osób bliskich, imion zwierząt, popularnych słów, typowych zestawów np. 123,
2. Użytkownik zobowiązuje się do zachowania hasła w poufności; nawet po utracie jego nieważności,
3. Hasła nie mogą być ujawniane innym osobom. Zabrania się zapisywania haseł na kartkach i w notesach, naklejania ich na komputerze, lub tablicy korkowej, trzymania w szufladzie lub pod klawiaturą,
4. Zapisane hasło musi być przechowywane w zamkniętej kopercie w sejfie,
5. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione,
6. Użytkownik zobowiązany jest do zmiany swojego hasła (nie rzadziej niż co 30 dni),
7. Użytkownik zobowiązany jest do samodzielnej zmiany hasła, jeżeli system tego nie wymusza,
8. Administrator zobowiązany jest do ustawienia zmiany hasła, jeżeli system mu to umożliwia,
9. Hasło użytkownika składa się z minimum 8 znaków; w tym duże i małe litery, cyfry i znaki specjalne.

16. OCHRONA ANTYWIRUSOWA:

1. Administrator Danych Osobowych zobowiązany jest do instalacji oprogramowania antywirusowego; w tym zapewnienia odpowiedniej ilości licencji na każdym komputerze,
2. System antywirusowy zapewnia ochronę systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej,
3. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada,
4. Zabrania się wyłączania systemu antywirusowego podczas pracy systemu informatycznego, przetwarzającego dane osobowe,
5. Użytkownik zobowiązany jest do niezwłocznego poinformowania administratora i inspektora ochrony danych osobowych, administratora sieci informatycznych w przypadku stwierdzenia zainfekowania systemu lub pojawiania się komunikatu o treści: „Twój system jest zainfekowany!", „Wykryto zagrożenie",
6. Aktualizacja definicji wirusów odbywa się automatycznie przez system.

17. ZASADY POSTĘPOWANIA W SYTUACJACH NARUSZENIA:

1. Wszystkie osoby upoważnione zobowiązane są do niezwłocznego powiadomienia administratora oraz inspektora ochrony danych osobowych o fakcie wystąpienia naruszenia,
2. Przed przystąpieniem do pracy, osoby upoważnione zobowiązane są do dokonania oceny i oględzin miejsca ich pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań, związanych z ochroną danych osobowych,
3. Do sytuacji wymagających powiadomienia należą:
   a) niewłaściwie zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
4. Do incydentów wymagających powiadomienia należą:
   a) Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   c) Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5. Typowe przykłady incydentów wymagające reakcji:

a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
b) dokumentacja jest niszczona bez użycia niszczarki,
c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
e) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia administratora,
g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
h) telefoniczne próby wyłudzenia danych osobowych,
i) kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi,
j) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
l) hasła do systemów przyklejone są w pobliżu komputera.

18. DODATKOWE DOKUMENTY:

Jako załączniki do regulaminu zostaną wprowadzone następujące dokumenty określające:

a) Wykaz miejsc przetwarzania danych osobowych,
b) Wykaz danych przetwarzanych przez administratora,
c) Wykaz zabezpieczeń stosowanych przez administratora.

19.ZAPISY KOŃCOWE:

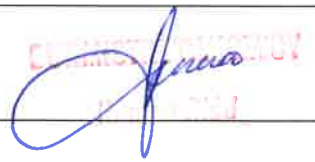
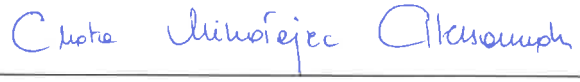
1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy,
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez administratora lub inspektora za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.
3. Z naruszenia obowiązków wynikających z niniejszego dokumentu lub z postępowania sprzecznego mogą zostać wyciągnięte konsekwencje dyscyplinarne w postaci pisemnego upomnienia, nagany lub kary finansowej. Do wyciągania konsekwencji prawo ma administrator oraz inspektor ochrony danych.

Aleksandra Cnota-Mikołajec

.....Inspektor Ochrony Danych.....
Inspektor Ochrony Danych

.....
Administrator Danych Osobowych

Załącznik do Regulaminu Ochrony Danych Osobowych

Nazwa podmiotu wprowadzającego	Urząd Miejski w Głuszycy
Data wprowadzenia	7 stycznia 2025 r.
Numer zarządzenia wprowadzającego Regulamin Ochrony Danych Osobowych	3/2025
Podpis ADO	
Podpis IOD	

1. Wykaz miejsc przetwarzania danych osobowych

L.p.	Miejsce przetwarzania danych osobowych	Adres	Ilość pomieszczeń
1.	Urząd Miejski w Głuszycy	ul. Parkowa 9, 58-340 Głuszyca	23
2.	Pomieszczenie w Budynku Firmy Informatycznej EMNET	ul. Sienkiewicza 7, 58-340 Głuszyca	1
3.	Centrum Przesiadkowe	ul. Łukasiewicza, 58-340 Głuszyca	1

2. Wykaz danych przetwarzanych przez administratora

L.p.	Rodzaj przetwarzanych danych	Sposób ich przetwarzania z określeniem programu, w którym dane są przetwarzane
1.	AKTA OSOBOWE	Wersja papierowa
2.	DANE PRACOWNICZE KADROWO-PŁACOWE	Wersja papierowa + wersja elektroniczna (FKA 2000, VULCAN, Bestia)

3.	DANE PRACOWNICZE DO ZUS	Wersja papierowa + wersja elektroniczna (FKA 2000, VULCAN, Bestia, Płatnik)
4.	DANE PRACOWNICZE DO URZĘDU SKARBOWEGO	Wersja papierowa + wersja elektroniczna (FKA 2000, VULCAN, Bestia)
5.	POLISY UBEZPIECZENIOWE	Wersja papierowa + wersja elektroniczna (FKA 2000)
6.	DANE DOT. ZAKŁADOWEGO FUNDUSZU ŚWIADCZEŃ SOCJALNYCH	Wersja papierowa + wersja elektroniczna (FKA 2000)
7.	DANE DOT. ŚWIADCZEŃ ZDROWOTNYCH	Wersja papierowa + wersja elektroniczna (FKA 2000)
8.	REJESTR FAKTUR	Wersja papierowa + wersja elektroniczna (FKA 2000)
9.	PROJEKTY FINANSOWANE ZE ŚRODKÓW ZEWNĘTRZNYCH	Wersja papierowa
10.	REJESTR SKARG I WNIOSKÓW	Wersja papierowa
11.	SPRAWY SĄDOWE I ADMINISTRACYJNE	Wersja papierowa
12.	UMOWY I UMOWY CYWILNOPRAWNE	Wersja papierowa
13.	DANE DOT. SZKOLEŃ PRACOWNIKÓW	Wersja papierowa
14.	DZIENNIK KORESPONDENCYJNY LUB POCZTOWA KSIĄŻKA NADAWCZA	Wersja papierowa + wersja elektroniczna (READY)
15.	DOWODY KSIĘGOWE	Wersja papierowa + wersja elektroniczna (FKA 2000, BESTIA)
16.	DANE DOT. AWANSU ZAWODOWEGO	Wersja papierowa
17.	DANE DO FUNDUSZU NAGRÓD	Wersja papierowa + wersja elektroniczna (FKA 2000)
18.	REJESTR WYPADKÓW LUB KSIĘGA WYPADKOWA	Wersja papierowa
19.	KSIĘGI STANU CYWILNEGO I INNE DANE USC	Wersja papierowa + wersja elektroniczna (ŹRÓDŁO)
20.	EWIDENCJA GRUNTÓW I BUDYNKÓW	Wersja papierowa + wersja elektroniczna (EWID)
21.	REJESTR MŁODZIEŻY SPEŁNIAJĄCEJ OBOWIĄZEK SZKOLNY ORAZ OBOWIĄZEK NAUKI	Wersja papierowa + wersja elektroniczna (SIO)
22.	REJESTR AKTÓW NADANIA STOPNIA AWANSU ZAWODOWEGO NAUCZYCIELI MIANOWANYCH	Wersja papierowa

23.	ARKUSZE ORGANIZACYJNE PLACÓWEK OŚWIATOWYCH	Wersja papierowa
24.	CZŁONKOWIE ZESPOŁÓW KRYZYSOWYCH	Wersja papierowa
25.	REJESTR BYŁYCH I AKTUALNYCH MIESZKAŃCÓW	Wersja papierowa + wersja elektroniczna (ELUD)
26.	EWIDENCJA WNIOSKÓW O WYDANIE DOWODU OSOBISTEGO	Wersja papierowa + wersja elektroniczna (ŹRÓDŁO)
27.	EWIDENCJA UTRACONYCH I WYDANYCH DOWODÓW OSOBISTYCH	Wersja papierowa + wersja elektroniczna (ŹRÓDŁO)
28.	KOPERTY DOWODOWE	Wersja papierowa + wersja elektroniczna (ŹRÓDŁO)
29.	WNIOSKI O PRZYZNANIE POMOCY MATERIALNEJ DLA UCZNIÓW ZAMIESZKAŁYCH NA TERENIE MIASTA	Wersja papierowa
30.	SIO	Wersja elektroniczna (SIO)
31.	OŚWIADCZENIA MAJĄTKOWE RADNYCH RADY MIEJSKIEJ	Wersja papierowa
32.	OŚWIADCZENIA MAJĄTKOWE DYREKTORÓW I KIEROWNIKÓW JEDNOSTEK ORGANIZACYJNYCH	Wersja papierowa
33.	PODATKI OD ŚRODKÓW TRANSPORTOWYCH	Wersja papierowa + wersja elektroniczna (FKA 2000)
34.	PODATEK ROLNY	Wersja papierowa + wersja elektroniczna (FKA 2000)
35.	PODATEK LEŚNY	Wersja papierowa + wersja elektroniczna (FKA 2000)
36.	KSIĘGOWOŚĆ PODATKOWA	Wersja papierowa + wersja elektroniczna (FKA 2000)
37.	PODATEK OD NIERUCHOMOŚCI	Wersja papierowa + wersja elektroniczna (FKA 2000)
38.	REJESTR PODMIOTÓW PODWYŻSZAJĄCYCH WARTOŚĆ WEKSLA	Wersja papierowa
39.	REJESTR WIECZYSTYCH UŻYTKOWNIKÓW I DZIERŻAWCÓW GRUNTÓW	Wersja papierowa + wersja elektroniczna (FKA 2000)
40.	ZAMÓWIENIA PUBLICZNE	Wersja papierowa
41.	WNIOSKI I UMOWY O NAJEM LOKALI UŻYTKOWYCH	Wersja papierowa
42.	EWIDENCJA DZIAŁALNOŚCI GOSPODARCZEJ	Wersja papierowa + wersja elektroniczna (CEiDG)

43.	REJESTR WNIOSKÓW O DZIERŻAWĘ GRUNTÓW ROLNYCH	Wersja papierowa
44.	WNIOSKI O PRZYDZIAŁ MIESZKAŃ KOMUNALNYCH	Wersja papierowa
45.	WNIOSKI O SPRZEDAŻ I ZAMIANĘ GRUNTÓW	Wersja papierowa
46.	WNIOSKI O UZGODNIENIE LOKALIZACJI INWESTICJI	Wersja papierowa
47.	WNIOSKI O WIECZYSTE UŻYTKOWANIE GRUNTÓW	Wersja papierowa
48.	WNIOSKI O ZEZWOLENIE NA ZAJĘCIE PASA DROGOWEGO	Wersja papierowa
49.	REJESTR DECYZJI O PODZIALE NIERUCHOMOŚCI	Wersja papierowa
50.	REJESTR DECYZJI O USTALENIE LOKALIZACJI CELU PUBLICZNEGO	Wersja papierowa
51.	REJESTR DECYZJI O WARUNKACH ZABUDOWY TERENU	Wersja papierowa
52.	OPINIE LOKALIZACYJNE	Wersja papierowa
53.	WNIOSKI DOTYCZĄCE PLANU ZAGOSPODAROWANIA PRZESTRZENNEGO	Wersja papierowa
54.	REJESTR OBYWATELI POLSKICH ZAMELDOWANYCH NA POBYT CZASOWY LUB STAŁY	Wersja elektroniczna (ELUD)
55.	REJESTR OBCOKRAJOWCÓW ZAMELDOWANYCH NA POBYT CZASOWY LUB STAŁY	Wersja elektroniczna (ELUD)
56.	REJESTR OSÓB I INSTYTUCJI, KTÓRE ZŁOŻYŁY WNIOSKI DOTYCZĄCE UDZIAŁU W PROJEKCIE ZAKUPU I MONTAŻU KOLEKTORÓW SŁONECZNYCH	Wersja papierowa
57.	REJESTR DECYZJI O ŚRODOWISKOWYCH UWARUNKOWANIACH ZGODY NA REALIZACJĘ PRZEDSIĘWZIĘCIA	Wersja papierowa
58.	WNIOSKI ROLNIKÓW PODSZKODOWANYCH DŁUGOTRWAŁĄ SUSZĄ	Wersja papierowa + wersja elektroniczna (FKA 2000)
59.	REJESTR ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH W POSTACI TRADYCYJNEJ	Wersja papierowa + wersja elektroniczna (CEiDG, FKA 2000)
60.	REJESTR PRACOWNIKÓW DO SPRAW OBRONY CYWILNEJ	Wersja papierowa
61.	WNIOSKI ROLNIKÓW O ZWROT PODATKU AKCYZOWEGO ZA ZAKUPIONY OLEJ NAPĘDOWY	Wersja papierowa + wersja elektroniczna (SRPP, FKA 2000)
62.	WNIOSKI ROLNIKÓW POSZKODOWANYCH W WYNIKU KLĘSKI ŻYWIOŁOWEJ	Wersja papierowa + wersja elektroniczna (FKA 2000)

63.	EWIDENCJA WYDANYCH DECYZJI NA WYCINKĘ DRZEW	Wersja papierowa
64.	REJESTR ZBIORNIKÓW BEZODPŁYWOWYCH I PRZYDOMOWYCH OCZYSZCZALNI ŚCIEKÓW	Wersja papierowa
65.	EWIDENCJA AZBESTU	Wersja papierowa
66.	REJESTR OSÓB WŁĄCZONYCH W REALIZACJĘ ZADAŃ OKRESU „W"	Wersja papierowa
67.	REJESTR UCZESTNIKÓW PROCESU INWESTYCYJNEGO	Wersja papierowa
68.	REJESTR CZŁONKÓW TERENOWYCH FORMACJI OC	Wersja papierowa
69.	REJESTR PRZEDPOBOROWYCH ORAZ LISTA POBOROWYCH	Wersja papierowa + wersja elektroniczna (ELUD)
70.	DODATKI MIESZKANIOWE	Wersja papierowa + wersja elektroniczna (RADIX NDM)
71.	REJESTR PŁATNIKÓW PODATKU VAT	Wersja papierowa + wersja elektroniczna (SYGNITY, FKA 2000)
72.	DANE KONTRAHENTÓW	Wersja papierowa + wersja elektroniczna (FKA 2000)
73.	REJESTR KONT OSOBISTYCH PRACOWNIKÓW URZĘDU, RADNYCH ORAZ SOŁTYSÓW	Wersja papierowa + wersja elektroniczna (FKA 2000)
74.	DANE OSOBOWE STAŻYSTÓW	Wersja papierowa + wersja elektroniczna (FKA 2000)
75.	DANE OSOBOWE WOLONTARIUSZY	Wersja papierowa
76.	DANE OSOBOWE PRAKTYKANTÓW	Wersja papierowa
77.	REJESTR WYBORCÓW	Wersja papierowa + wersja elektroniczna (ELUD, Źródło CRW)
78.	REJESTR UCHWAŁ RADY MIEJSKIEJ	Wersja elektroniczna
79.	REJESTR INTERPELACJI	Wersja papierowa + wersja elektroniczna
80.	REJESTR ZAPYTAŃ W TRYBIE DOSTĘPU DO INFORMACJI PUBLICZNEJ	Wersja elektroniczna
81.	REJESTR OSÓB PRZYSTĘPUJĄCYCH DO KONKURSÓW NA STANOWISKA DYREKTORÓW I KIEROWNIKÓW JEDNOSTEK ORGANIZACYJNYCH	Wersja papierowa
82.	DOKUMENTACJA ZWIĄZANA Z OCENĄ RYZYKA ZAWODOWEGO	Wersja papierowa

83.	REJESTR ZAMIESZKANIA CUDZOZIEMCÓW	Wersja elektroniczna (ELUD)
84.	REJESTR OPINII PRAWYCH	Wersja papierowa
85.	MONITORING WIZYJNY MIASTA I URZĘDU	Wersja elektroniczna
86.	KARTA DUŻEJ RODZINY	Wersja papierowa
87.	ZESPÓŁ INTERDYSCYPLINARNY	Wersja papierowa
88.	EGZEKUCJA ADMINISTRACYJNA	Wersja papierowa + wersja elektroniczna (ETW, KRD, PRS, FKA 2000)
89.	REJEST PRZYZNANYCH ULG W ZOBOWIĄZANIACH	Wersja papierowa + wersja elektroniczna (SHRIMP, SRPP)
90.	AKTY NOTARIALNE	Wersja papierowa
91.	GMINNA KOMISJA ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH	Wersja papierowa
92.	DOFINANSOWANIE DO WYPOCZYNKU DZIECI I UCZNIÓW	Wersja papierowa + wersja elektroniczna (VULCAN)
93.	SPADKOBIERCY	Wersja papierowa + wersja elektroniczna (FKA 2000)
94.	WINDYKACJA	Wersja papierowa + wersja elektroniczna (ETW, PRS, FKA 2000)
95.	REJESTR SPRZEDAŻY NIERUCHMOŚCI	Wersja papierowa
96.	DANE ŁAWNIKÓW	Wersja papierowa
97.	REJESTR PETYCJI	Wersja elektroniczna
98.	GOSPODARKA ODPADAMI KOMUNALNYMI	Wersja papierowa
99.	UPOMNIENIA I TYTUŁY WYKONAWCZE	Wersja papierowa + wersja elektroniczna (ETW, FKA 2000)
100.	NUMERACJA PORZĄDKOWA NIERUCHOMOŚCI	Wersja papierowa + wersja elektroniczna (EWID, GEOSYSTEM)
101.	REJESTR OSÓB KTÓRYM PRZYZNANO DODATEK OSŁONOWY	Wersja papierowa + wersja elektroniczna (SYGNITY)
102.	WYKAZ CZŁONKÓW JEDNOSTEK OCHOTNICZEJ STRAŻY POŻARNEJ	Wersja papierowa

103.	BUDŻET OBYWATELSKI	Wersja papierowa
104.	PRACOWNICY WYKONAWCÓW PRAC NA TERENIE MIASTA	Wersja papierowa
105.	PODATEK OD OSÓB FIZYCZNYCH	Wersja papierowa + wersja elektroniczna (FKA 2000)
106.	PODATEK OD SPADKÓW I DAROWIZN	Wersja papierowa + wersja elektroniczna (FKA 2000)
107.	REJESTR OSÓB KTÓRYM PRZYZNANO ŚWIADCZENIE WYCHOWAWCZE	Wersja papierowa + wersja elektroniczna (SYGNITY)
108.	DOKUMENTACJA DOTYCZĄCA OCHRONY MAŁOLETNICH	Wersja papierowa
109.	DOKUMENTACJA DOTYCZĄCA OBSŁUGI ZGŁOSZEŃ SYGNALISTÓW	Wersja papierowa

3. Wykaz zabezpieczeń stosowanych przez administratora

L.p.	Rodzaj zabezpieczenia	Zabezpieczenie fizyczne / techniczne / organizacyjne
1.	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).	Zabezpieczenie fizyczne
2.	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.	Zabezpieczenie fizyczne
3.	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.	Zabezpieczenie fizyczne
4.	Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.	Zabezpieczenie fizyczne
5.	Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.	Zabezpieczenie fizyczne
6.	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.	Zabezpieczenie fizyczne
7.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.	Zabezpieczenie fizyczne
8.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.	Zabezpieczenie fizyczne

9.	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej.	Zabezpieczenie fizyczne
10.	Pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.	Zabezpieczenie fizyczne
11.	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.	Zabezpieczenie fizyczne
12.	Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.	Zabezpieczenie techniczne
13.	Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.	Zabezpieczenie techniczne
14.	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	Zabezpieczenie techniczne
15.	Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.	Zabezpieczenie techniczne
16.	Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.	Zabezpieczenie techniczne
17.	Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	Zabezpieczenie techniczne
18.	Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	Zabezpieczenie techniczne
19.	Użyto system Firewall do ochrony dostępu do sieci komputerowej.	Zabezpieczenie techniczne
20.	Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.	Zabezpieczenie techniczne
21.	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	Zabezpieczenie techniczne
22.	Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.	Zabezpieczenie techniczne
23.	Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.	Zabezpieczenie techniczne

24.	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.	Zabezpieczenie techniczne
25.	Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	Zabezpieczenie techniczne
26.	Pliki przesyłane elektronicznie są szyfrowane za pomocą programu 7 – ZIP.	Zabezpieczenie techniczne
27.	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.	Zabezpieczenie organizacyjne
28.	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.	Zabezpieczenie organizacyjne
29.	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.	Zabezpieczenie organizacyjne
30.	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.	Zabezpieczenie organizacyjne

Aleksandra Cnota-Mikołajec
Inspektor Ochrony Danych
.....
Inspektor Ochrony Danych

.....
Administrator Danych Osobowych

Zał. Nr 2 do Zarządzenie Nr 3/0/2025 z dnie 7.01.25r.

Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych

Rozdział 1.

Postanowienia ogólne

§ 1

1. Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku, gdy:

   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,

   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych.

2. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie, jest wyznaczony przez administratora danych osobowych – inspektor ochrony danych.

Rozdział 2.

Tryb i zasady postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego

§ 2

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym administratora danych osobowych oraz inspektora ochrony danych.
2. Inspektor ochrony danych po otrzymaniu powiadomienia:

   1) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł),

   2) zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,

   3) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,

   4) niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,

   5) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

6) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu (włamaniu do systemu), opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

3. Raport wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) inspektor ochrony danych przekazuje administratorowi danych osobowych jednostki.
4. Inspektor ochrony danych w porozumieniu z administratorem danych osobowych podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu w przyszłości.

Rozdział 3.

Tryb postępowania w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych

§ 3

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązana jest niezwłocznie powiadomić o tym inspektora ochrony danych lub inną upoważnioną przez niego osobę.
2. Inspektor ochrony danych po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):

   1) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

   2) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),

   3) sprawdza jakość komunikacji w sieci telekomunikacyjnej,

   4) sprawdza zawartość zbioru danych osobowych,

   5) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

3. W przypadku stwierdzenia naruszenia zabezpieczeń danych:

   1) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, blokuje dostęp do sieci telekomunikacyjnej, do programów oraz zbiorów danych itp.),

   2) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,

   3) niezwłocznie przywraca prawidłowy stan działania systemu,

   4) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia,

   5) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie), inspektor ochrony danych przekazuje administratorowi danych osobowych jednostki.
5. Inspektor ochrony danych, w porozumieniu z administratorem danych osobowych, podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągniecie konsekwencji prawem przewidzianych.

Rozdział 4.

Postanowienia końcowe

§ 4

1. Każda osoba wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zobowiązana jest do zapoznania się z niniejszą instrukcją. Wykonanie powyższego zobowiązania pracownik potwierdza własnoręcznym podpisem.
2. Wszelkie zmiany niniejszej instrukcji skutkują wobec osób, których dotyczą, z dniem ich doręczenia na piśmie.

7.01.2025 r. Aleksandra Cnota-Mikołajec Inspektor Ochrony Danych

Data i podpis inspektora ochrony danych

Oświadczam, że zostałem/am zapoznany z instrukcją postępowania w sytuacji naruszenia systemu ochrony danych osobowych i jej postanowienia akceptuję własnoręcznym podpisem

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....
7. .....
8. .....
9. .....
10. .....
11. .....
12. .....
13. .....
14. .....
15. .....
16. .....
17. .....
18. .....
19. .....
20. .....
21. .....
22. .....
23. .....
24. .....
25. .....
26. .....
27. .....
28. .....
29. .....
30. .....
31. .....
32. .....
33. .....
34. .....
35. .....
36. .....
37. .....
38. .....
39. .....
40. .....
41. .....
42. .....
43. .....

44. .....
45. .....
46. .....
47. .....
48. .....
49. .....
50. .....
51. .....
52. .....
53. .....
54. .....
55. .....
56. .....
57. .....
58. .....
59. .....
60. .....
61. .....
62. .....
63. .....
64. .....
65. .....
66. .....
67. .....
68. .....
69. .....
70. .....
71. .....
72. .....
73. .....
74. .....
75. .....
76. .....
77. .....
78. .....
79. .....
80. .....
81. .....
82. .....
83. .....
84. .....
85. .....
86. .....
87. .....
88. .....
89. .....
90. .....

Zał. Nr 3 do Zarządzenie
Nr 3/0/2025 z 7.01.25 r.

Rejestr naruszeń ochrony danych osobowych

Nazwa podmiotu wprowadzającego	Urząd Miejski w Głuszycy
Data wprowadzenia	7 stycznia 2025 r.
Numer zarządzenia wprowadzającego	3/2025
Podpis ADO	
Podpis IOD	Chata Milczejec Aleksandra

Na podstawie art. 33 oraz 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)

wprowadza się w Urzędzie Miejskim w Głuszycy,

dokument o nazwie „Rejestr naruszeń ochrony danych osobowych", zwanym dalej „Rejestr naruszeń"

§1

Podstawowe definicje:

1) **Incydent (naruszenie)** – jest to pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań jednostki i zagrażają bezpieczeństwu informacji,
2) **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
3) **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie

poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

4) **Ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,
5) **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
6) **Identyfikator użytkownika** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
7) **Hasło** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
8) **Poufność danych** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§2

W przypadku wystąpienia naruszenia przepisów o ochronie danych osobowych, Administrator Danych Osobowych lub Inspektor Ochrony Danych, zobowiązani są bez zbędnej zwłoki (w miarę możliwości, lecz nie później niż w terminie 72 godzin po stwierdzeniu naruszenia) zgłosić naruszenie organowi nadzorczemu właściwemu. Jeśli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator Danych Osobowych lub Inspektor Ochrony Danych są zwolnieni z informowania organu nadzorczego właściwego.

§3

Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

§4

Każda osoba upoważniona w Urzędzie Miejskim w Głuszycy bez zbędnej zwłoki zgłasza Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych, fakt wystąpienia naruszenia.

§5

Jeśli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

§6

Zawiadomienie, o którym mowa w §2, nie jest wymagane, gdy:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności

środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt a),

c) Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

.....

Administrator Danych Osobowych

Aleksandra Cnota-Mikołajec
Inspektor Ochrony Danych
.....

Inspektor Ochrony Danych

Przykłady naruszeń

1. Najczęściej pojawiającym się incydentem jest niewłaściwie zaadresowana poczta elektroniczna. Typowe jest korzystanie z przydatnej funkcji zapamiętywania adresów w programie pocztowym. W założeniach ma ona pomóc w wyeliminowaniu błędów, jakie pojawiają się przy ręcznym wprowadzaniu adresu odbiorcy. Okazuje się jednak, że użytkownicy często tracą czujność i nie sprawdzają podpowiadanego przez program adresu mailowego. Może to spowodować wysłanie wiadomości do niewłaściwego adresata. Konsekwencje mogą być różne w zależności od treści przesłanej wiadomości.

2. Kolejnym incydentem jaki występuje w wielu jednostkach są grupy nośników znikające z naszych zasobów, takie jak zwykłe kartki, teczki, czy też segregatory z danymi. Do incydentów związanych z ich utratą dochodzi najczęściej w siedzibie podmiotu, np. w wyniku niefrasobliwości pracowników, którzy pozostawiają osoby postronne bez nadzoru w miejscach, gdzie takie dane są łatwo dostępne. Pozostawianie dokumentów na widoku również może powodować przykre konsekwencje, jakie wiążą się ze złożeniem skargi przez petenta.

3. Nieco rzadziej występującym incydentem jest utrata (zgubienie, kradzież) telefonu, laptopa, pamięci przenośnej, a nawet torby czy teczki z danymi w wersji papierowej. W przypadku kradzieży sprzętu elektronicznego, skupiamy się najczęściej jedynie na utracie materialnej wartości sprzętu, nie zwracając uwagi na dane, które się na nim znajdowały. Dopiero później pojawiają się obawy o bezpieczeństwo danych i wątpliwości, czy twardy dysk laptopa jest szyfrowany lub czy można zdalnie usunąć dane z telefonu komórkowego. Dużym problemem dla poszkodowanego podmiotu może być brak właściwej kontroli nad sprzętem. Dodatkowo incydentem jest brak pisemnego upoważnienia do korzystania ze sprzętu służbowego poza terenem jednostki.

4. Udostępnienie danych osobowych budzi coraz więcej pytań i wątpliwości. Kiedy można je udostępnić? Komu udostępnić i na jakiej podstawie? Powszechnie uznaje się, że udostępnienie danych polega na wręczeniu komuś kartki papieru zawierającej dane osobowe. W praktyce jednak ta forma występuje już niezwykle rzadko. Najczęściej przekazywanie danych następuje poprzez zdalne dostępy przydzielane niekiedy bezterminowo (np. pracownikom czy działowi IT). Należy przy tym pamiętać, aby udostępniać poszczególne dane tylko tym osobom, które faktycznie na nich pracują, a także aby odbierać dostęp tym, którzy już go nie potrzebują, np. byłym pracownikom.

5. Poza elektronicznym dostępem do danych, popularny jest również kanał telefoniczny. W dobie wyłudzeń informacji z wykorzystaniem różnego rodzaju socjotechnik, telefon jest obecnie najbardziej niebezpiecznym urządzeniem do przekazywania danych. Wyobraźmy

sobie, że nasz rozmówca przedstawia się jako urzędnik skarbowy lub inspektor UODO i prosi nas o różne dane. Wiele osób w takich sytuacjach dane po prostu przekazuje, bez wcześniejszej weryfikacji rozmówcy. Dodatkowo częstym procederem jest informowanie osób postronnych o zwolnieniach lekarskich jednego z pracowników jednostki.

6. Powszechną praktyką w niemal każdej firmie jest wyrzucanie podręcznych notatek, czy nawet dokumentów do zwykłych koszy na śmieci. Niektórzy zdają się myśleć, że kilkukrotne przedarcie kartki sprawi, że z danego dokumentu nic nie będzie można odczytać. Gdyby jednak tak było, zapewne nie powstały niszczarki do dokumentów. Tymczasem okazuje się, że nawet w podmiotach, które dysponują niszczarkami, korzysta się z nich rzadko. Warto wiedzieć, że dane przechowywane w wersji papierowej muszą być pod kontrolą również wówczas, gdy są niszczone.

Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania naprawcze

Raport z naruszenia ochrony danych

1. Data ..... Godzina .....
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):
    a. .....
    b. .....
    c. .....
    d. .....
3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie stanowiska roboczego, nazwa programu lub aplikacji itp.):
    a. .....
    b. .....
    c. .....
    d. .....
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
    a. .....
    b. .....
    c. .....
    d. .....
5. Podjęte działania:
    a. .....
    b. .....
    c. .....
    d. .....
6. Wstępna ocena przyczyn wystąpienia naruszenia:
    a. .....
    b. .....
    c. .....
    d. .....
7. Postępowanie wyjaśniające i naprawcze:
    a. .....
    b. .....
    c. .....
    d. .....

.....

(podpis pracownika)

.....

(data i podpis IOD)

Zał. Nr 4 do Zarządzenia
Nr 3/0/2025 z dnia 7.01.25 r.

Rejestr udostępnień danych osobowych

L.p.	Podmiot lub osoba, której udostępniono dane osobowe	Data udostępnienia	Miejsce udostępnienia danych	Zakres i cel udostępnienia danych	Na podstawie wniosku z dnia	Osoba udostępniająca dane	Sposób udostępnienia (papierowo lub elektronicznie (jaki nośnik)
1.							
2.							
3.							
4.							
5.							
6.							